Report on Present State of OK-ECDSA and OK-ECDH Evaluation (screening evaluation)

January 28, 2002

Atsushi Shimbo, Member

Public-Key Cryptography Subcommittee

OK-ECDSA
(submitter’s claims)

- Category: Signature
- Security basis: Discrete logarithm problem on
  Montgomery-form elliptic curve
- Provable security: The scheme is the unmodified ECDSA scheme.
  It has no established proof of security.

  (The submitter cites Brown’s results using a generic group model.)
- Characteristics:
  - Strong ability to withstand side channel attacks
  - Well-suited to IC card implementations; uses only a small amount of memory when running.
- SW implementation information:
  Signature generation: 11.0ms; signature verification: 21.6msec
  (Pentium III 866MHz)

OK-ECDH

(submitter's claims)

- Category: Key agreement
- Security basis: Discrete logarithm problem on
  Montgomery-form elliptic curve
- Provable security: The scheme is the unmodified ECDH scheme.
  Although there are no security proofs,
  the scheme is heuristically believed to be
  secure against passive attacks.
- Characteristics:
  - Strong ability to withstand side channel attacks
  - Well-suited to IC card implementations; uses only a small amount of memory when running.
- SW implementation information: Key agreement: 11.0ms
  (Pentium III 866MHz)

OK-ECDSA and OK-ECDH Technical Characteristics

- Use of randomized projective coordinates on Montgomery-form elliptic curve
  - Same calculation sequence, regardless of secret information
  - Values to be calculated are randomized.
- Introduction of technique for reproducing Y coordinate in Montgomery-form elliptic curve addition (without using Y coordinate)
- The schemes are the unmodified ECDSA and ECDH schemes
  - The only differences are at the primitive implementation level.
- Montgomery-form elliptic curves are a restricted class of elliptic curves, but approximately 40% of general elliptic curves can be transformed into the Montgomery-form.

Screening evaluation

- OK-ECDSA and OK-ECDH have common technical characteristics, so the same three evaluators were requested to evaluate them.
- Cryptographic technique specifications:
  - No unclear or questionable points.
  - Some feel the recommended values for the elliptic curve parameters are missing (partially).
- Self-evaluation
  - Comments are concentrated on the ability to withstand side channel attacks.

Evaluation comments

- Ability to withstand side channel attacks not sufficiently evaluated
  - The claim that these schemes have a strong ability to withstand side channel attacks seems justified, but there is not quantitative evaluation based on implementations.
  - The evaluations of the submitter are only theoretical observations. Because issues at the implementation level were not discussed, there is a possibility that implementations could have poor ability to withstand side channel attacks.
  - Implementations of these schemes need to be compared to other techniques. In addition, the schemes must be evaluated with consideration for platform characteristics and computation cycles.
  - The same applies to the amount of required memory.
  - There are no smart card implementation evaluation results.
  - The grounds for the hardware implementation results are not presented.